UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

TRICIA GARNETT, individually and on behalf all other similarly situated,

Plaintiff,

Case No. 22-cv-1225

v.

HOPE COLLEGE,

Defendant.

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Tricia Garnett ("Plaintiff") brings this Class Action Complaint against Hope College ("Hope College" or "Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and alleges as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant Hope College, a private college located in Holland, Michigan. Defendant failed to implement and maintain reasonable data security measures, such as standard encryption or redaction of sensitive data, leading to the theft of the sensitive personal information of Plaintiff and other current and former students, admission applicants, employees of Hope College, and others who entrusted Defendant with their most sensitive data. Plaintiff seeks damages on behalf of herself and Class Members, as well as equitable relief, including, without limitation, injunctive relief designed to protect the sensitive information of Plaintiff and Class Members.

2. This action arises from Defendant's failure to properly secure and safeguard the

unencrypted and unredacted data of at least 156,713 individuals.[1]

3. Before and through September 27, 2022, Defendant obtained Plaintiff's and Class Members' personally identifiable information ("PII") and stored that PII, unencrypted, in an Internet-accessible environment on Defendant's network.

4. On or about December 15, 2022, Hope College notified state Attorneys General and many Class Members about a widespread data breach in which the sensitive PII of individuals was accessed and acquired by a malicious actor. Hope College explained in a notice letter that on September 27, 2022, it "discovered potential unauthorized access to our network" and that an investigation later determined that "certain data … may have been subject to unauthorized access." (the "Data Breach").[2]

5. The PII that was exfiltrated in the Data Breach includes, but is not limited to, names, dates of birth, Social Security numbers, driver's license numbers, and Student ID numbers.[3]

6. According to Hope College's posted cyber security update on its website, as well as the Notice Letter it sent Attorneys General and some Class Members, Hope College "discovered potential unauthorized access to its network," worked with its IT team and "third-party forensic and legal specialists" and engaged in a "full forensic investigation" to determine the scope and cause of the Data Breach.[4]

7. The Notice Letter plainly admits that Plaintiff's and Class Members' PII was compromised, stating that "third-party specialists determined that certain sensitive information

[1] Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/9574bf0a-94d2-4653-8665-da79a7728b4b.shtml (last accessed Dec. 26, 2022).
[2] Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/9574bf0a-94d2-4653-8665-da79a7728b4b/7a50da1a-1609-4b27-af7b-ab04401d29a6/document.html (last accessed Dec. 23, 2022) (hereafter "Notice Letter")
[3] Hope College Cyber Security Update, https://hope.edu/_resources/cybersecurityupdate.pdf (last accessed Dec. 23, 2022)
[4] *Id.*

kept in the normal course of business may have been subject to unauthorized access."[5] This means that Plaintiff's and Class Members' PII was likely exfiltrated (i.e., actually accessed) by the unauthorized actors during the Data Breach.

8. Plaintiff and Class Members first learned of the September 2022 Data Breach when they received Data Breach notice letters via regular U.S. mail directly from Hope College.

9. In its Notice Letters, sent to state and federal agencies and some Class Members, Hope College does not explain the precise scope of the Data Breach or how long the unauthorized actor had access to Defendant's network.[6]

10. The letter provides no further information regarding the Data Breach and only goes on to recommend how victims can place a fraud alert or credit freeze on their account and how to sign up for the identity monitoring services Defendant offered in response to the Data Breach. The letters Plaintiff and other Class Members received do not explain how the Data Breach occurred, what steps Hope College took following the Data Breach, whether Hope College made any changes to its data security, or most importantly, whether Plaintiff's PII remains in the possession of criminals.

11. Plaintiff's and Class Members' unencrypted, unredacted PII was compromised due to Hope College's negligent and/or careless acts and omissions, and due to its utter failure to protect Class Members' sensitive data. Hackers targeted and obtained the PII because of its value in exploiting and stealing the identities of Plaintiff and similarly situated Class Members. The risks to these persons will remain for their respective lifetimes.

12. Defendant failed to undertake adequate cybersecurity practices, including but not limited to, maintaining the PII in an unencrypted format and failing to adhere to routine

[5] *Id.*
[6] *Id.*

cybersecurity protocols and procedures.

13. Plaintiff brings this action on behalf of all persons whose PII was compromised due to Hope College's failure to: (i) adequately protect Plaintiff's and Class Members' PII; (ii) warn Plaintiff and Class Members of its inadequate information security practices; and (iii) effectively monitor Hope College's network for security vulnerabilities and incidents. Hope College's conduct amounts at least to negligence and violates federal and state statutes.

14. Plaintiff and Class Members have suffered injuries due to Hope College's conduct. These injuries include: (i) lost or diminished value of PII; (ii) loss of privacy (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (v) the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits; deal with spam messages and e-mails received subsequent to the Data Breach, (vi) charges and fees associated with fraudulent charges on their accounts, and (vii) the present, continued, and certainly an increased risk to their PII, which remains in Hope College's possession and is subject to further unauthorized disclosures so long as Hope College fails to undertake appropriate and adequate measures to protect the PII. These risks will remain for the lifetimes of Plaintiff and Class Members.

15. Hope College disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or at the very least negligently, failing to take and implement adequate and reasonable measures to ensure that Class Members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable,

required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As the result, Plaintiff's and Class Members' PII was compromised through disclosure to unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

I. PARTIES

Plaintiff Garnett

16. Plaintiff Tricia Garnett is a resident and citizen of Arizona, residing in Chandler, Arizona. Plaintiff Garnett is a former Hope College student. Hope College mailed a Data Security Incident letter, dated December 15, 2022, by U.S. Mail, to Plaintiff's attention. The letter was sent to Plaintiff Garnett's mother's address.

Defendant Hope College

17. Defendant Hope College is a private liberal arts college located in Holland, Michigan and has a principal place of business at 141 East 12th St., Holland, Michigan 49423.

18. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

19. All of Plaintiff's claims stated herein are asserted against Hope College and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns responsible for the acts alleged herein.

II. JURISDICTION AND VENUE

20. This Court has original subject-matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d). First, because the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs. Second, because this class action involves a putative class of over 100 members. And third, because there is sufficient diversity—while Defendant's principal place of business is in Michigan, many Class Members, including Plaintiff Tricia Garnett, are citizens of different states.

21. This Court has general personal jurisdiction over Defendant because Defendant's principal place of business is in Michigan, and Defendant regularly conducts business in Michigan, and is primarily located in Holland, Michigan.

22. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, Defendant conducts substantial business in this District, and Defendant is located in Holland, Michigan.

III. FACTUAL ALLEGATIONS

Background

23. Defendant Hope College is a private liberal arts college. There are approximately 3,251 students currently enrolled at Hope College. Yet, Hope College has inexplicably collected, stored, and failed to protect the highly sensitive PII of over more than 156,000 individuals.

24. In its Notice Letters sent to Attorneys General, Hope College claims that it "take[s] the privacy and security of the information in [its] care seriously, and sincerely regret[s] any worry or inconvenience this incident may cause…"[7]

[7] *Id*.

25. Plaintiff and the Class Members, as current or former students, applicants, or employees of Hope College, reasonably relied (directly or indirectly) on this sophisticated higher education institution to keep their sensitive PII confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII. People demand security to safeguard their PII, especially when Social Security numbers are involved as here.

26. Hope College had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties and as evidenced by the Data Breach, it failed to adhere to that duty.

Defendant Fails to Secure the PII, Resulting in a Data Breach

27. On or around December 15, 2022, Hope College first began notifying Class Members and state Attorneys General ("AGs") about a widespread breach of its computer systems and involving the sensitive personal identifiable information of Plaintiff and Class Members. Hope College explained that the Data Breach was detected on September 27, 2022.[8]

28. After detecting the Data Breach, Hope College "immediately began working with its IT team, and third-party forensic and legal specialists… to conduct a full forensic investigation" of Hope College's systems. The "investigation" determined that Plaintiff's and Class Members' PII (including but not limited to full names and Social Security numbers) may have been copied and acquired by unauthorized persons at the time of the incident. [9]

29. Defendant states that it "sincerely regret[s] any worry or inconvenience this incident may cause" to Plaintiff and Class Members and their families.[10] Then, Defendant told the

[8] *Id.*
[9] *Id.*
[10] *Id.*

victims of the Data Breach to direct their concerns and questions to a call center—that is closed on weekends and holidays, and only open during select hours on weekdays.[11]

30. Upon information and belief, Plaintiff and Class Members in this action were, current, former, and prospective students at Hope College, their parents, and Hope College employees. Hope College has still not disclosed to Plaintiff and Class Members the full scope of the Data Breach or precisely what information was impacted, or whether the exfiltrated PII remains under the control of the cyber criminals who took it.

31. According to the Notice Letter, the confidential information that was potentially accessed without authorization included at least first and last names in combination with Social Security numbers, date of birth, driver's license numbers, and Student ID numbers.

32. Upon information and belief, the PII was not encrypted prior to the data breach.

33. Upon information and belief, the cyberattack was targeted at Hope College as a higher education institution that collects and maintains valuable personal, health, tax, and financial data.

34. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) Plaintiff's and Class Members' PII.

35. Hope College admitted in its Notice Letter to the Attorneys General that it only discovered the unauthorized access in September 2022. In the Notice Letters, Hope College made no indication of when the improper access began or was terminated, who committed the cyber-attack, what the degree of access to Plaintiff and Class Members' PII was, or whether Hope College knows what information was actually compromised as opposed to potentially compromised.[12]

[11] *Id.*
[12] *See Id.*

36. With its offer of credit and identity monitoring services to victims, Hope College is acknowledging that the impacted persons are subject to an imminent threat of identity theft and financial fraud as a result of its failure to protect the PII it collected and maintained.

37. In response to the Data Breach, Hope College fails to speak to the vulnerabilities in its cybersecurity systems and networks, and further fails to provide any assurances that steps will be made to better secure Plaintiff's and Class Members' PII going forward.[13]

38. Hope College had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep the PII that was entrusted to Hope College confidential, and to protect the PII from unauthorized access and disclosure.

39. Plaintiff and Class Members provided their PII to Hope College with the reasonable expectation that Hope College, as a higher education institution, would comply with its duties, obligations, and representations to keep such information confidential and secure from unauthorized access.

40. Hope College failed to uphold its data security obligations to Plaintiff and Class Members. As a result, Plaintiff and Class Members are significantly harmed and will be at a high risk of identity theft and financial fraud for many years to come.

41. Hope College did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining, causing Plaintiff's and Class Members' PII to be exposed.

42. As explained by the Federal Bureau of Investigation, "[p]revention is the most

[13] *Id*.

effective defense against ransomware and it is critical to take precautions for protection."[14]

43. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs,

[14] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed Aug. 23, 2021).

including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[15]

44. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….
- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) ….
- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….
- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up

[15] *Id.* at 3-4.

to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[16]

45. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

-Apply latest security updates
-Use threat and vulnerability management
-Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

-Monitor for adversarial activities
-Hunt for brute force attempts
-Monitor for cleanup of Event Logs
-Analyze logon events

[16] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last accessed Aug. 23, 2021).

Harden infrastructure

-Use Windows Defender Firewall
-Enable tamper protection
-Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[17]

46. Given that Defendant was storing the PII of thousands of individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

47. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of thousands of individuals, including Plaintiff and Class Members.

Securing PII and Preventing Breaches

48. Hope College could have prevented this Data Breach by properly encrypting or otherwise protecting its equipment and computer files containing PII.

49. In its notice letters, Hope College acknowledged the sensitive and confidential nature of the PII. To be sure, collection, maintaining, and protecting PII is vital to virtually all of Hope College's business purposes as a private higher education institution. Hope College acknowledged through its conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law it may not disclose and must take reasonable steps to protect PII from improper release or disclosure.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

[17] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last accessed Aug. 23, 2021).

50. Defendant recently disclosed to the Maine Attorney General that the Data Breach was the result of an SQL injection.[18] "SQL injection is one of the most common web hacking techniques."[19] "A successful SQL injection attack can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information. Many high-profile data breaches in recent years have been the result of SQL injection attacks, leading to reputational damage and regulatory fines. In some cases, an attacker can obtain a persistent backdoor into an organization's systems, leading to a long-term compromise that can go unnoticed for an extended period."[20]

51. "The majority of SQL injection vulnerabilities can be found quickly and reliably …. SQL injection can be detected manually by using a systematic set of tests against every entry point in the application…. Most instances of SQL injection can be prevented by using parameterized queries (also known as prepared statements) instead of string concatenation within the query." [21]

52. It is also well known that PII, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

53. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[22]

---

[18]https://apps.web.maine.gov/online/aeviewer/ME/40/9574bf0a-94d2-4653-8665-da79a7728b4b.shtml (last visited Dec. 27, 2022).
[19] https://www.w3schools.com/sql/sql_injection.asp (last visited Dec. 27, 2022).
[20] https://portswigger.net/web-security/sql-injection (last visited Dec. 27, 2022).
[21] *Id.*
[22] Bree Fowler, *Data breaches break record in 2021*, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last visited Oct. 11, 2022).

54. "Since 2005, K–12 school districts and colleges/universities across the US have experienced over 1,850 data breaches, affecting more than 28.6 million records."[23]

55. In 2020 alone, approximately 2.99 million records from educational institutions were subject to data breaches.[24]

56. Before this Data Breach occurred, Forbes published an article in April 2022 titled "Cyberattacks Pose 'Existential Risk' to Colleges-And Sealed One Small College's Fate."[25] The Forbes article noted that data breaches "are becoming more frequent" for higher education institutions, in part because "[h]igher education institutions have historically underfunded cybersecurity efforts, and the environment of information sharing and different computer systems across departments combine to make colleges and universities prime targets for cyber criminals." *Id*. Furthermore, Forbes identified a slew of colleges and universities that experienced data breaches between January 2022 and April 2022 (when the article was published) including North Carolina A&T State University, North Orange County Community College District, Ohlone Community College District, and Midland University. Accordingly, data breaches in the higher education sector are entirely foreseeable and indeed was foreseeable to Hope College. *Id*.[26]

57. Individuals place a high value not only on their PII, but also on the privacy of that data. For the individual, identity theft causes "significant negative financial impact on victims" as

---

[23] Sam Cook, US schools leaked 28.6 million records in 1,851 data breaches since 2005, https://www.comparitech.com/blog/vpn-privacy/us-schools-data-breaches/ (last accessed Oct. 11, 2022).

[24] *Id.*

[25] https://www.forbes.com/sites/emmawhitford/2022/04/19/cyberattacks-pose-existential-risk-to-colleges-and-sealed-one-small-colleges-fate/?sh=14f6bbda53c2 (last visited on Oct. 27, 2022).

[26] Furthermore, Marymount Manhattan College experienced a data breach in November 2021. https://www.mmm.edu/offices/information-technology/cybersecurity/ (Last visited on Oct. 27, 2022). Savannah College of Art & Design experienced a data breach in August 2022. https://apps.web.maine.gov/online/aeviewer/ME/40/9dd9255f-ff64-4ce3-80db-f70ebf4b1d9e.shtml (last accessed on Dec. 26, 2022).

well as severe distress and other strong emotions and physical reactions.

58. Individuals are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers." There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their Social Security numbers have been accessed, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."

59. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Hope College knew or should have known that its electronic records would be targeted by cybercriminals.

60. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

61. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite their own acknowledgment of its duties to keep PII private and secure, Hope College failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

62. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks, including

ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

63. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[27]

64. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "***[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies***. They breach networks, use specialized tools to maximize damage, ***leak corporate information on dark web portals***, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[28]

65. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that ***"[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data*** if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[29]

66. This readily available and accessible information confirms that, prior to the Data

---

[27] FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), *available at* https://www.ic3.gov/Media/Y2019/PSA191002 (last accessed Jan. 25, 2022).

[28] ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), *available at* https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last accessed Jan. 25, 2022).

[29] U.S. CISA, Ransomware Guide – September 2020, *available at* https://www.cisa.gov/sites/default/files/publications/CISA_MS ISAC_Ransomware%20Guide_S508C_.pdf (last accessed Jan. 25, 2022).

Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

67. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of thousands of individuals in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and Defendant's type of business had cause to be particularly on guard against such an attack.

68. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Hope College.

69. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

At All Relevant Times Hope College Had a Duty to Plaintiff and Class Members to Properly Secure their PII

70. At all relevant times, Hope College had a duty to Plaintiff and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to promptly notify Plaintiff and Class Members when Hope College became aware that their PII may have been compromised.

71. Hope College's duty to use reasonable security measures arose as a result of the

special relationship that existed between Hope College, on the one hand, and Plaintiff and the Class Members, on the other hand. The special relationship arose because Plaintiff and the Members of the Class entrusted Hope College with their PII as a condition of receiving educational services for themselves including applying for admittance to Hope College or when they applied for or accepted employment at Hope College.

72. Hope College had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Hope College breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

73. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

74. The Federal Trade Commission ("FTC") defines identity theft as "a fraud

committed or attempted using the identifying information of another person without authority."[30] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[31]

75. The ramifications of Hope College's failure to keep Plaintiff's and Class Members' PII secure are long lasting and severe. Once PII is stolen, particularly Social Security numbers as here, fraudulent use of that information and damage to victims is likely to continue for years.

The Value of PII

76. Stolen personal information is one of the most valuable commodities on the information black market. According to Experian, a credit-monitoring service, stolen personal information can sell for over $1,000.00 (depending on the type of information).[32]

77. The value of Plaintiff's and Class Members' personal information on the black market is considerable. Stolen personal information trades on the black market for years, and criminals frequently post stolen PII openly and directly on various "dark web" internet websites. Thus, after charging a substantial fee, criminals make such stolen information publicly available.

78. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[33] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker

[30] 17 C.F.R. § 248.201 (2013).
[31] *Id*.
[32] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.
[33] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

who in turn aggregates the information and provides it to marketers or app developers.[34]

79. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its acquisition by cybercriminals. This transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is likely readily available to others, and the rarity of the PII has been destroyed, thereby causing additional loss of value.

80. By failing to properly notify Plaintiff and the Class Members of the Data Breach, Defendant exacerbated their injuries. Specifically, by depriving them of the chance to take speedy measures to protect themselves and mitigate harm, Defendant allowed their injuries to fester and the damage to spread.

81. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[35]

82. Furthermore, trying to change or cancel a stolen Social Security number is no minor

[34] *See* https://datacoup.com/ (last accessed Oct. 21, 2022).
[35] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Dec. 10, 2021).

task. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

83. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[36]

84. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[37]

85. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[38]

86. It can take years for victims to notice their identity was stolen—giving criminals plenty of time to sell one's personal information to the highest bidder.

87. One example of criminals using PII for profit is the development of "Fullz" packages.

---

[36] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed Dec. 10, 2021).

[37] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Dec. 10, 2021).

[38] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

88. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members.

89. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

90. That is exactly what is happening to Plaintiff and Class Members. And it is reasonable for any trier of fact, including this Court or a jury, to find that the stolen PII (of Plaintiff and the other Class Members) is being misused—and that such misuse is fairly traceable to Defendant's data breach.

91. Over the past several years, data breaches have become alarmingly common. In 2016, the number of data breaches in the U.S. exceeded 1,000—a 40% increase from 2015.[39] The next year, that number increased further by nearly 45%.[40]

92. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets—so that they are aware of, and prepared for, a potential attack. One report explained that smaller entities "are attractive to ransomware criminals . . . because they often have lesser IT defenses and a

[39] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RESOURCE CENTER (Jan. 19, 2017), https://bit.ly/30Gew91 [hereinafter "*Data Breaches Increase 40 Percent in 2016*"] (last accessed Aug. 15, 2022).

[40] *Data Breaches Up Nearly 45 Percent According to Annual Review by Identity Theft Resource Center® and CyberScout®*, IDENTITY THEFT RESOURCE CENTER (Jan. 22, 2018), https://bit.ly/3jdGcYR [hereinafter "*Data Breaches Up Nearly 45 Percent*"] (last accessed Aug. 15, 2022).

high incentive to regain access to their data quickly."[41]

93. Thus, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry—including Defendant.

94. Responsible for handling highly sensitive personal information, Defendant knew or should have known the importance of safeguarding PII. Defendant also knew or should have known of the foreseeable consequences of a data breach. These consequences include the significant costs imposed on victims of the breach. Still, Defendant failed to take adequate measures to prevent the data breach.

95. Because of Defendant's inadequate practices, the PII of Plaintiff and the Class was exposed to criminals. In other words, Defendant opened up, disclosed, and then exposed its PII to crooked operators and criminals. Such criminals engage in disruptive and unlawful business practices and tactics, like online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud)—all using stolen PII.

96. Given the nature of Hope College's Data Breach it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' PII can easily obtain Plaintiff's and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

97. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, simple credit card information in a

[41] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last accessed Aug. 15, 2022).

retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[42] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

98. To date, Hope College has offered Plaintiff and Class Members *only one year* of credit monitoring services from their discovery of the Data Breach to the Notice Letters. The offered services are inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

99. The injuries to Plaintiff and Class Members were directly and proximately caused by Hope College's failure to implement or maintain adequate data security measures to protect PII that it maintained.

Hope College Failed to Comply with FTC Guidelines

100. Federal and State governments have established security standards and issued recommendations to lessen the risk of data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[43]

101. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and

[42] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, *available at*: https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed Dec. 10, 2021).

[43] Federal Trade Commission, *Start With Security, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Dec. 10, 2021).

practices for business.[44] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

102. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[45]

103. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks

[44]Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed Dec. 10, 2021).
[45] FTC, *Start with Security*, *supra* note 59.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

104. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

105. Because Class Members entrusted Hope College with their PII directly or indirectly, Hope College had, and has, a duty to the Class Members to keep their PII secure.

106. Plaintiff and the other Class Members reasonably expected that when they provided PII to Hope College that such PII would be protected and safeguarded.

107. Hope College was at all times fully aware of its obligation to protect the personal data of Students, including Plaintiff and members of the Classes. Hope College was also aware of the significant repercussions if it failed to do so.

108. Hope College's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data—including Plaintiff's and Class Members' full names, Social Security numbers, and other highly sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Plaintiff and Class Members Have Suffered Concrete Injury As A Result Of Defendant's Inadequate Security And The Data Breach It Allowed.

109. Plaintiff and Class Members reasonably expected that Defendant would provide adequate security protections for their PII, and Class Members provided Defendant with sensitive personal information, including their Social Security numbers.

110. Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant for their education, Plaintiff and other Class Members reasonably understood and expected that their PII would be protected with data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected. As such, Plaintiff and the Class Members suffered pecuniary injury.

111. Cybercriminals target and capture PII to exploit it; the Class Members are now, and for the rest of their lives will be, at a heightened risk of identity theft. Plaintiff have also incurred

(and will continue to incur) damages in the form of, *inter alia*, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

112. The cybercriminals who targeted and obtained Plaintiff's and Class Members' PII may exploit the information they obtained by selling the data in so-called "dark markets." Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;
- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

113. In addition, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

114. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and the other Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

115. Furthermore, certain PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.[46]

[46] *Id.*

116. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[47] Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[48] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[49] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

117. As a result of the Data Breach, Plaintiff and Class Members have already suffered damages.

Plaintiff Garnett's Experience

118. On or around December 15, 2022, Plaintiff Tricia Garnett, a citizen and resident of Arizona, reviewed a letter titled Notice of Data Security Incident letter sent by U.S. Mail to Plaintiff's mother's address. The letter Plaintiff received was substantially similar to those provided to the Attorneys General, but still lacked any detail about the scope of the Data Breach, the means of attack, or what specific steps that Defendant took in response to the Data Breach. The letter did disclose that Plaintiff's first and last name, date of birth, and Social Security number

---

[47] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (Feb. 23, 2012), http://www.iii.org/insuranceindustryblog/?p=267 (last accessed Dec. 10, 2021).

[48] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php (last accessed Dec. 10, 2021).

[49] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, (*available at* https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf) (last accessed Dec. 10, 2021).

were compromised in the Data Breach.

119. Plaintiff provided her PII when applying for admission to Hope College in 2007. She provided her PII for the purpose of gaining admission and qualifying for financial aid. In exchange, Plaintiff reasonably understood that Hope College would adequately safeguard her PII and delete her PII after it no longer had a legitimate use for it.

120. As a result of the Data Breach and the information that she received in the letter, Plaintiff has spent many hours dealing with the consequences of the Data Breach (considering closing and opening bank accounts, changing banks, changing passwords, and now self-monitoring her bank and credit accounts), as well as her time spent verifying the legitimacy of the Notice Letter, communicating with her bank, and exploring credit monitoring and identity theft insurance options. This time has been lost forever and cannot be recaptured and time that she could have spent on other pursuits like work or leisure activities.

121. Plaintiff is very careful about sharing her own personal identifying information and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

122. Plaintiff stores any and all documents containing PII in a secure location, and destroys any documents she receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

123. Plaintiff suffered actual injury in the form of damages and diminution in the value of her PII, a form of intangible property that she entrusted to Hope College, which was compromised in and as a result of the Data Breach.

124. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and she has suffered anxiety and increased concerns for the theft of her privacy

since she received the Notice Letter. She is especially concerned about the theft of her full name paired with her date of birth, and Social Security number.

125. Plaintiff suffered concrete injury from the loss of her privacy.

126. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

127. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Hope College's possession, is protected and safeguarded from future breaches.

IV. CLASS ALLEGATIONS

128. Plaintiff brings this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

129. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **All persons Defendant identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

130. Excluded from the Class are the following individuals and/or entities: Hope College, and Hope College's parents, subsidiaries, affiliates, officers and directors, and any entity in which Hope College has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

131. Plaintiff reserves the right to modify or amend the definition of the proposed class and any future subclass before the Court determines whether certification is appropriate.

132. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of thousands of individuals whose sensitive data was compromised in Data Breach. Defendant reported to the Attorney General of Maine that the Data Breach affected 156,713 individuals.[50]

133. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PII;

f. Whether Defendant breached its duty to Class Members to safeguard their PII;

g. Whether Defendant knew or should have known that its data security systems

[50] https://apps.web.maine.gov/online/aeviewer/ME/40/9574bf0a-94d2-4653-8665-da79a7728b4b.shtml

and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breach implied contracts with Plaintiff and Class Members;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

134. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach.

135. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

136. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

137. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

138. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

139. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Hope College would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

140. The litigation of the claims brought herein is manageable. Hope College's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

141. Adequate notice can be given to Class Members directly using information maintained in Hope College's records.

142. Unless a Class-wide injunction is issued, Hope College may continue in its failure to properly secure the PII of Class Members, Hope College may continue to refuse to provide proper notification to Class Members regarding the Data Breach, the PII Hope College continues to maintain will remain at risk of future breach, and Hope College may continue to act unlawfully as set forth in this Complaint.

143. Further, Hope College has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive relief with regard to the Class Members as a whole is appropriate.

144. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws,

regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and/or

h. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

145. Plaintiff and Class Members incorporate the above allegations as if fully set forth herein.

146. Plaintiff and Class Members entrusted their PII to Defendant. Defendant owed to Plaintiff and other Class Members a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the data breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

147. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with industry standards concerning data security would result in the compromise of that PII —just like the Data

Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

148. Defendant owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the data breach. This duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the data breach.

149. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and Class Members' PII.

150. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

151. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class Members and the importance of exercising reasonable care in handling it.

152. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal

information and PII of Plaintiff and Class Members—which actually and proximately caused the Data Breach and injured Plaintiff and Class Members.

153. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

154. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the data breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

155. Plaintiff and Class Members incorporate the above allegations as if fully set forth herein.

156. Plaintiff brings this claim for unjust enrichment in the alternative to Plaintiff's claims for breach of contract.

157. Plaintiff and Class Members conferred a monetary benefit on Defendant in the form of monetary payments—directly or indirectly—for providing education or employment to current and former students and employees.

158. Plaintiff and Class Members also conferred a monetary benefit on Defendant in the form of their PII, from which Defendant derived revenue as it could not provide education, employment, or services without the use of that PII.

159. Defendant collected, maintained, and stored Plaintiff and Class Members' PII and, as such, Defendant had knowledge of the monetary benefits it received on behalf of the Plaintiff and Class Members.

160. The money that Plaintiff and Class Members paid to Defendant, or the revenue Defendant derived from the use of their PII, should have been used to pay, at least in part, for the administrative costs and implementation of data security adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII. Additionally, employees conferred a monetary benefit on Defendant as part of their salary and benefits was intended to apply to adequate data security which Defendant did not apply.

161. Defendant failed to implement—or adequately implement—those data security practices, procedures, and programs to secure sensitive PII, as evidenced by the Data Breach.

162. As a result of Defendant's failure to implement data security practices, procedures, and programs to secure sensitive PII, Plaintiff and Class Members suffered actual damages in an amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiff's PII.

163. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement the data security measures adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII.

164. As a direct and proximate result of Defendant's decision to profit rather than provide adequate security, and Defendant's resultant disclosures of Plaintiff's and Class Members' PII, Plaintiff and Class Members suffered and continue to suffer considerable injuries in the forms of time and expenses mitigating harms, diminished value of PII, loss of privacy, and a present increased risk of harm.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

165. Plaintiff and Class Members incorporate the above allegations as if fully set forth herein.

166. Plaintiff's and Class Members' PII was provided to Defendant as part of education services or employment that Defendant provided to Plaintiff and Class Members.

167. Plaintiff and Class Members agreed to pay Defendant tuition for education and administration services. Additionally, applicants for admission or employment agreed to provide their PII in exchange for Defendant's promise to keep it safe from unauthorized access.

168. Defendant and Plaintiff and Class Members entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning the security of Plaintiff's and Class Members' PII, whereby, Defendant was obligated to take reasonable steps to secure and safeguard Plaintiff's and Class Members' PII.

169. Defendant had an implied duty of good faith to ensure that the PII of Plaintiff and Class Members in its possession was only used in accordance with its contractual obligations.

170. Defendant was therefore required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiff's and Class

Members' PII and to comply with industry standards and applicable laws and regulations for the security of this information.

171. Defendant breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiff's and Class Members' PII, resulting in the Data Breach.

172. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

173. As a result of Defendant's conduct, Plaintiff and Class Members did not receive the full benefit of the bargain.

174. Had Defendant disclosed that its data security was inadequate, neither Plaintiff or Class Members, nor any reasonable person would have entered into such contracts with Defendant.

175. As a result of Data Breach, Plaintiff and Class Members suffered actual damages resulting from the theft of their PII, as well as the loss of control of their PII, and remain at present risk of suffering additional damages.

176. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and all Class Members, request judgment against the Hope College and that the Court grant the following:

A. For an Order certifying the Class and appointing Plaintiff and her Counsel to represent the Class;

B. For equitable relief enjoining Hope College from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and

the Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to the Plaintiff and the Class;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including but not limited to an order:

i. prohibiting Hope College from engaging in the wrongful and unlawful acts described herein;

ii. requiring Hope College to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Hope College to delete, destroy, and purge the personal identifying information of Plaintiff and Class unless Hope College can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and the Class;

iv. requiring Hope College to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff's and Class Members' personal identifying information;

v. prohibiting Hope College from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

vi. requiring Hope College to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Hope

College's systems on a periodic basis, and ordering Hope College to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Hope College to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Hope College to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Hope College to segment data by, among other things, creating firewalls and access controls so that if one area of Hope College's network is compromised, hackers cannot gain access to other portions of Hope College's systems;

x. requiring Hope College to conduct regular database scanning and securing checks;

xi. requiring Hope College to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Hope College to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Hope College to implement a system of tests to assess its respective

employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Hope College's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Hope College to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Hope College's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Hope College to meaningfully educate all class members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Hope College to implement logging and monitoring programs sufficient to track traffic to and from Hope College's servers;

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Hope College's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: December 27, 2022

Respectfully Submitted,

/s/ Charles R. Ash, IV

Charles R. Ash, IV (P73877)
ASH LAW, PLLC
402 W. Liberty St.
Ann Arbor, MI 48178
Phone: 734-234-5583
cash@nationalwagelaw.com

Terence R. Coates*
Justin C. Walker*
Dylan J. Gould*
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
jwalker@msdlegal.com
dgould@msdlegal.com

Attorneys for Plaintiff and the Proposed Class

**admission applications forthcoming*